РЕЦЕНЗІЯ

професора кафедри комп'ютерних систем, мереж та кібербезпеки
Національного університету біоресурсів і природокористування України,
доктора технічних наук, професора **КРИВОРУЧКО Олени Володимирівни**
на дисертацію **ГЛАЗУНОВА Андрія Сергійовича** на тему:
«Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах»,
подану на здобуття ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки»
галузі знань 12 «Інформаційні технології»

Обґрунтування вибору теми дослідження. Дисертацію присвячено актуальній науково-прикладній проблемі виявлення зовнішніх порушників у хмарних сервісах, значущість якої суттєво зростає в умовах стрімкого розвитку хмарних обчислень, обробки великих обсягів даних та підвищення інтенсивності кіберзагроз. Обрана тематика відповідає напрямам розвитку спеціальності 122 «Комп'ютерні науки», зокрема у частині розроблення інтелектуальних методів аналізу даних, моделей прийняття рішень та забезпечення інформаційної безпеки розподілених систем.

В дисертації коректно визначено об'єкт і предмет дослідження, а також чітко й логічно сформульовано мету та основні завдання, що забезпечує концептуальну цілісність і внутрішню узгодженість подання матеріалу дисертації. Методичний підхід до розв'язання задачі виявлення інсайдерів ґрунтується на її інтерпретації як задачі баєсівського послідовного прийняття рішень в умовах невизначеності. Такий підхід дозволяє формалізувати процес обробки невизначених і неповних даних, враховувати ймовірнісні залежності між ознаками загроз та реалізовувати алгоритмічні процедури оцінювання ризиків у хмарному середовищі. Запропоновані в роботі підходи узгоджуються з сучасними тенденціями розвитку інтелектуальних систем, машинного навчання та ймовірнісного моделювання, що підтверджує їх релевантність і перспективність для подальшого наукового та практичного застосування.

Ступінь обґрунтованості наукових результатів дисертації, їх достовірності та новизни. Дисертація відзначається високим рівнем системності, логічною послідовністю викладу матеріалу та належним ступенем обґрунтованості всіх етапів дослідження: від ґрунтовного аналізу предметної області до апробації отриманих результатів. Це свідчить про цілісний характер проведеного дослідження та достатній рівень його наукової аргументованості. Достовірність отриманих результатів забезпечується використанням математичного апарату, зокрема баєсівських підходів до моделювання та прийняття рішень в умовах невизначеності, а також узгодженістю теоретичних положень із результатами їх практичної перевірки.

Наукова новизна дисертаційного дослідження полягає у тому, що:

вперше:

– розроблено модифіковану модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах інформаційних систем, яка, на відміну від існуючих підходів, передбачає використання спеціалізованих вузлів для моделювання потенційно шахрайських дій осіб, що обіймають керівні посади, а також враховує цифрові сліди, сформовані під час взаємодії з хмарними застосунками, що дає змогу здійснювати оцінювання ймовірності внутрішньої загрози ще до виникнення безпекового інциденту;

– запропоновано структуру зазначеної моделі з формалізованим описом апріорних та апостеріорних ймовірностей подій, що відповідають ключовим індикаторам інформаційної безпеки, яка, на відміну від відомих аналогів, інтегрує як технічні параметри, так і поведінкові характеристики користувача, забезпечуючи підвищення точності раннього виявлення інсайдерів у хмарному середовищі;

удосконалено:

– метод виявлення несанкціонованого доступу до хмарних сервісів шляхом впровадження адаптивної баєсівської мережі з функцією прогнозування інсайдерської загрози, що, на відміну від існуючих рішень, враховує причинно-наслідкові залежності між індикаторами ризику в умовах невизначеності та забезпечує можливість своєчасної ідентифікації загрози до її реалізації з метою мінімізації потенційних збитків;

– процедуру побудови оптимальних послідовних баєсівських правил шляхом урахування нелінійних залежностей між імовірністю реалізації інциденту та оцінками ризику, що сприяє більш точній адаптації алгоритмів прийняття рішень у сфері інформаційної безпеки хмарних сервісів;

набув подальшого розвитку метод раннього виявлення інсайдерів в організаціях, що використовують хмарні сервіси, який, на відміну від існуючих підходів, одночасно враховує технічні, поведінкові та організаційні характеристики користувачів, і орієнтований на зниження ймовірності несанкціонованого доступу з боку співробітників, зокрема тих, які мають розширені повноваження, зокрема на керівних посадах.

Викладені положення підтверджуються експериментальними результатами, апробацією на міжнародних конференціях (Міжнародній науково-практичній конференції молодих вчених «Інформаційні технології: економіка, техніка, освіта ‘2023» (м. Київ, 2023 р.); XII Міжнародній науково-практичній конференції «Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2024» (м. Київ, 2024 р.) та у виданнях, включених до Переліку наукових фахових видань України.

Значення одержаних результатів для науки і практики та рекомендації щодо їх можливого використання. Практичне значення дисертаційного дослідження полягає

у розробленій програмній реалізації та апробації інтелектуальної моделі виявлення інсайдерських загроз у хмарних середовищах з використанням модифікованої баєсівської мережі, що дає змогу здійснювати багатофакторну оцінку ризику, пов'язаного з поведінкою співробітників, які взаємодіють із хмарними сервісами, зокрема з урахуванням можливих шахрайських дій з боку осіб, які займають керівні посади. У свою чергу, розроблена модифікована модель баєсівської мережі для виявлення інсайдерських загроз у хмарних сервісах дозволяє формалізувати процес прийняття рішень в умовах невизначеності та враховувати причинно-наслідкові залежності між індикаторами ризику. Модель баєсівської мережі та розроблені алгоритми прогнозування загроз можуть інтегруватися у сучасні хмарні системи інформаційної безпеки як інструмент раннього попередження, що дозволяє мінімізувати потенційні фінансові та операційні збитки. Результати дослідження можуть стати методичною основою для розроблення спеціалізованого програмного забезпечення та експериментальних систем моніторингу поведінки користувачів у хмарних середовищах, можуть бути використані як у дослідженнях, так і в практичних розробках у сфері інформаційної безпеки підприємства (акт впровадження результатів дисертаційного дослідження у виробничий процес ТОВ «Інфобіт») та в освітньому процесі.

Оцінка змісту дисертації, її завершеності в цілому і оформлення. Дисертація Андрія Глазунова є завершеним науковим дослідженням, що відзначається цілісністю, логічною структурою та високим рівнем теоретичного й методологічного опрацювання. Робота має наступні складові: анотацію, вступ, три розділи, висновки, список використаних джерел та додатки. Загальний обсяг роботи становить 190 сторінок комп'ютерного тексту. Матеріал ілюстровано 11 таблицями та 37 рисунками. До дисертації також включено 3 додатки. Бібліографічний список містить 153 джерела, з яких 131 – іншомовні (латиницею).

У **вступі** обґрунтовано актуальність теми, визначено мету і завдання дослідження, окреслено об'єкт, предмет і методи, розкрито наукову новизну та практичне значення отриманих результатів. Також наведено відомості про апробацію результатів, публікаційну активність здобувача та структуру дисертації.

У **першому розділі** дисертаційного дослідження проведено огляд хмарних моделей та сервісів у різних галузях; проведено аналіз досліджень проблематики забезпечення інформаційної безпеки хмарних інфраструктур та аналіз методів машинного навчання, які потенційно можна використовувати для забезпечення безпеки хмарних сервісів. Зазначено особливості виявлення внутрішніх порушників інформаційної безпеки хмарних сервісів на основі методів машинного навчання. Доведено, що методи машинного навчання дають змогу аналізувати великі обсяги даних для виявлення аномалій у поведінці співробітників, а, відповідно, мережі Баєса – використовують для моделювання ймовірності того, що конкретний співробітник є потенційним порушником.

Другий розділ містить огляд методів та моделей виявлення інсайдерських загроз та застосування Баєсівського методу раннього виявлення інсайдерів в організаціях, які використовують хмарні послуги. Доведено (вперше), що запропонована модель мережі Баєса є корисною службі інформаційної безпеки під час виявлення внутрішніх порушників і відрізняється від аналогічних рішень тим, що в ній врахована загроза шахрайства особи, яка перебуває на керівній посаді в компанії, що використовує хмарні сервіси.

Третій розділ присвячено впровадженню стратегії перевірки гіпотез і мінімізації ризику неправильного визначення внутрішнього порушника під час роботи з хмарними сервісами. Зокрема показано, що баєсівські правила враховують різні фактори, такі як попередні аномалії, динаміку зміни ознак. Доповнено модель для розрахунку ймовірності інсайдерської загрози, яка, на відміну від існуючих досліджень, дає можливість також оцінювати шахрайські дії на керівних посадах компанії. Виконано розроблення і тестування мережі Баєса для моделювання внутрішнього порушника безпеки за допомогою програмного забезпечення GeNIe/SMILE, а також алгоритмічної мови Python

У **висновках** узагальнено основні наукові результати, сформульовано теоретичні та практичні положення, що відповідають поставленій меті та завданням дослідження, а також окреслено напрями подальших наукових досліджень.

Робота відзначається послідовністю викладу матеріалу, чіткою внутрішньою організацією та обґрунтованістю отриманих наукових результатів. Усі розділи дисертації логічно взаємопов’язані і спрямовані на досягнення сформульованої мети дослідження, що забезпечує її цілісність. Дисертація оформлена відповідно до вимог МОН України та характеризується завершеністю, високою культурою наукового викладу й відповідає критеріям кваліфікаційної праці на здобуття ступеня доктора філософії зі спеціальності 122 «Комп’ютерні науки».

Повнота викладення наукових положень, висновків і рекомендацій в наукових публікаціях, зарахованих за темою дисертації. Положення дисертації опубліковано у 6 наукових працях, з яких 4 статті у наукових виданнях, включених до Переліку наукових фахових видань України, 2 тези наукових доповідей. Основний внесок за обсягом у матеріалах публікацій належить здобувачу

Відсутність (наявність) порушення академічної доброчесності. Дисертація є самостійно виконаною кваліфікаційною науковою працею, у якій викладено обґрунтовані наукові положення, висновки та рекомендації, запропоновані автором для публічного захисту. Використання результатів, ідей та текстів інших авторів супроводжується посиланнями на відповідні джерела. Ознак привласнення чужих наукових результатів, ідей чи текстів без належного цитування не виявлено, що свідчить про дотримання принципів академічної доброчесності.

Дискусійні положення та зауваження щодо дисертації. Дисертація Андрія Глазунова виконана на високому науково-технічному рівні, відповідає спеціальності 122 «Комп'ютерні науки», має завершений характер. Водночас дисертація містить окремі дискусійні положення та зауваження, що не знижують її загальної наукової цінності, однак можуть бути враховані для подальшого вдосконалення дослідження.

1. В окремих фрагментах роботи доцільно уточнити та уніфікувати вживання термінів, зокрема таких як «угнута функція» та «угнутість функції», що сприятиме підвищенню термінологічної чіткості та однозначності трактувань.

2. Доцільним видається більш детальне обґрунтування вибору параметрів і структури запропонованої баєсівської мережі, зокрема в частині формування апріорних ймовірностей, джерел даних для їх оцінювання, а також процедур навчання та адаптації моделі, що дозволило б підвищити відтворюваність результатів і практичну придатність розробленого підходу.

3. Потребує розширення порівняльний аналіз запропонованого підходу з існуючими методами виявлення інсайдерських загроз у хмарних середовищах, зокрема із використанням кількісних метрик ефективності (точність, повнота, F-міра тощо), а також оцінювання обчислювальної складності та масштабованості алгоритмів, що є важливим з огляду на практичне впровадження в умовах великих даних.

4. У рисунках та схемах доцільно чітко зазначити особистий внесок автора (наприклад, «розроблено автором»), що відповідає вимогам до оформлення наукових праць та підвищує прозорість представлення результатів.

5. У роботі наявні окремі редакційні недоліки, зокрема описки, стилістичні неточності (зокрема на с. 66, 94–95, 107), а також окремі описки у підписах до рисунків.

Висловлені зауваження мають рекомендаційний характер і спрямовані на підвищення рівня формалізації, відтворюваності результатів, їх експериментальної валідації та практичної цінності в контексті сучасних задач комп'ютерних наук.

Загальний висновок. Загалом дисертація Андрія Глазунова на тему: «Комп'ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах» є завершеним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають важливе значення для розвитку методів виявлення інсайдерських загроз у хмарних сервісах та інформаційних системах. Зміст дисертації відповідає обраній темі, поставленій меті та сформульованим завданням. Отримані результати характеризуються науковою новизною, теоретичною обґрунтованістю та практичною цінністю, а також мають потенціал для подальшого розвитку і впровадження у сфері комп'ютерних наук та інформаційної безпеки. За рівнем наукової новизни, обґрунтованості отриманих результатів, їх достовірності та практичної значущості дисертація відповідає вимогам, що висуваються до дисертацій за спеціальністю 122 «Комп'ютерні науки».

Вважаю, що дисертація на тему: «Комп’ютерні баєсівські моделі виявлення інсайдерів у хмарних сервісах» повністю відповідає вимогам наказу Міністерства освіти і науки України № 40 від 12 січня 2017 року «Про затвердження вимог до оформлення дисертації» (зі змінами), Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України № 44 від 12 січня 2022 року (зі змінами), а її автор Глазунов Андрій заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп’ютерні науки» галузі знань «Інформаційні технології».

Рецензент професор кафедри комп’ютерних систем, мереж та кібербезпеки Національного університету біоресурсів і природокористування України, доктор технічних наук, професор Олена КРИВОРУЧКО